QuickStart for ServiceWatch

ServiceNow QuickStart implementations offer customers the ability to quickly implement specific ServiceNow applications. The QuickStart for ServiceWatch includes modeling of up to 10 business services, visualization of business service health and population and reconciliation of discovered Configuration Items (CIs) into Customer provided Configuration Management Database (CMDB). ServiceNow professional services consultants will work with the customer to implement ServiceWatch in a hosted environment as described below.

QuickStart Implementation Project Overview

The QuickStart includes services to implement ServiceWatch and integrate it into Customer's CMDB and event monitoring software. The following is a list of project tasks completed during this QuickStart:

Project Task	Description
Project Kick-off and Planning	Meetings to establish prerequisites and plan to complete them before the implementation and business service modeling can begin. Establish project schedule and task details.
Implementation and Business Service Modeling	Configuration of ServiceWatch, installation of collectors and discovery and modeling of 10 supported business services in Customer's environment.
CMDB Integration and CI Reconciliation	Integrate ServiceWatch to existing Customer's CMDB. Populate discovered CIs and relationships with each other. Existing CIs reconciled with discovered CIs.
Event Monitoring Integration	Integration with up to 3 event monitoring tools and/or event consoles to receive events and event properties. Store and manage events in ServiceWatch.
Event Binding and Impact Configuration	Configure event binding rules in ServiceWatch and define how the overall service health is calculated from the incoming events and CI status.
Dashboard Configuration	Configuration of ServiceWatch dashboard to provide single view into business service health including drill down to event and CI data to assist in root cause analysis.

ServiceWatch Configuration

As part of this project, ServiceNow will discover and model ten (10) business services using ServiceWatch. The business services models that will be discovered and generated as a part of this QuickStart will include the following details:

- Application components of the business service and relationships between them
- Servers upon which the discovered application components run
- Network infrastructure that supports the business services including layer 2 connectivity between each application component of the business service
- Virtualization layer and components that support the business service components
- Other topological constructs such as server farms and operating system clusters

QuickStart Project Roadmap and Deliverables

Project Kick-off and Planning

ServiceNow will conduct a project kick-off meeting to discuss the QuickStart prerequisites (see below). Additional planning meetings may be scheduled to ensure that the prerequisites are met before the implementation can begin. The result of these planning meetings will be a project plan including:

1. All project tasks, task ownership and dependencies
2. Project schedule
3. Detailed deployment plan including number of required ServiceWatch collector servers, placement of ServiceWatch collector servers and network and security considerations

Implementation and Business Service Modeling

ServiceNow will provision a ServiceWatch instance in a hosted environment. ServiceNow will conduct a virtual meeting session (using Webex or compatible conferencing software) to assist Customer in installing the ServiceWatch collector software and to validate credentials. The goal of this session is to verify that all of the required QuickStart prerequisites have been met by the Customer.

During the QuickStart, ServiceNow will use the ServiceWatch discovery engine to model ten (10) supported business services. Supported business services must include only items listed in the "ServiceWatch - Supported Systems and Applications" guide available on the ServiceNow Wiki. Models will include the following details:

- Application components of the business service and relations between them
- Servers upon which the above application components run
- Network infrastructure that supports the business services including layer 2 connectivity between each two application components of the business service
- Virtualization layer and components that support the business service components
- Other topological constructs such as server farms and operating system clusters

CMDB Integration and CI Reconciliation

ServiceNow will integrate ServiceWatch with one (1) Customer owned and previously implemented CMDB from this list:

- ServiceNow CMDB
- HP uCMDB

For each business service modeled, ServiceWatch will populate CIs and their relationships with other CIs to the integrated CMDB. Host and network CIs from ServiceWatch will be automatically reconciled with the equivalent existing CIs in the Customer CMDB based on predefined rules. Reconciliation of discovered applications with application CIs residing within the CMDB will be done according to the out of the box capabilities. If integrating to the ServiceNow CMDB, ServiceNow will demonstrate to Customer how to manage the CI reconciliation rules and CI type/attribute mapping in ServiceWatch.

ServiceWatch discovers hosts and network devices, but does not populate them to the Customer CMDB. Host and network device entries in the Customer CMDB are the responsibility of Customer.

Event Monitoring Integration

ServiceWatch will be integrated with up to three (3) Customer provided and previously implemented monitoring tools and/or event consoles that are accessible from ServiceWatch. These integrations will use existing ServiceWatch integrations listed in the "ServiceWatch - Supported Monitoring Tools" guide available on the ServiceNow Wiki. If the Customer monitoring tool or event console is not supported by an existing ServiceWatch integration, Customer must configure their monitoring tool or event console to send an SNMP trap to ServiceWatch.

Event Binding and Impact Configuration

ServiceNow will conduct a working session with Customer to define event binding (association) rules and impact tree settings for CIs discovered by ServiceWatch. ServiceNow will configure ServiceWatch to define service health calculation based on incoming events and CI status. ServiceNow will demonstrate how to configure ServiceWatch with Customer defined notification rules, notification message content, and message distribution and enable Customer to make additional configurations.

Dashboard Configuration

ServiceNow will conduct a working session with Customer to configure the ServiceWatch dashboard to aggregate the reporting into a single view. The dashboard will be configured to display business service health (as calculated from the incoming events) and provide capability to drill down into specific business service topologies in order to explore potential problem root causes.

ServiceNow Provided Resources

ServiceNow will provide the following resources for the project:

ServiceNow Resource	Responsibilities
Engagement Manager	Lead project planning, provide implementation expertise, follow the QuickStart deployment project plan, allocate appropriate resources from ServiceNow, and act as a single point of contact. Facilitate weekly status calls to track the target project progress.
Technical Consultant	Undertake the application configuration and integration and assist with knowledge transfer to Customer.

Required Customer Resources

Customer will provide the following resources and make them available throughout the duration the project (note that multiple responsibilities may be filled by the same Customer personnel):

Customer Resource	Responsibilities
Project Manager	Responsible for the project and meet regularly with the ServiceNow engagement manager to review progress and resolve issues.
Event Management Administrator	Resources with technical expertise to establish integrations with monitoring tools and/or event consoles.
CMDB Administrator	Resource with technical expertise to establish integration with CMDB.
Business Service Owner(s)	Subject matter expert(s) responsible for the correct and complete definition of the business services and underlying technical architecture to be modeled in ServiceWatch.

Customer Resource	Responsibilities
Security Team Member	Security team member capable of making decisions regarding necessary credentials and permissions to allow ServiceWatch to operate

QuickStart Prerequisites

Customer must meet all requirements listed in **Exhibit – ServiceWatch Implementation Prerequisites**, attached herein, and the following:

Business Services

Modeled business services must comprise of systems and applications supported by ServiceWatch as listed in the ”ServiceWatch - Supported Systems and Applications” guide available on the ServiceNow Wiki.

ServiceWatch Collector Server Requirements

This QuickStart will support the installation of up to three (3) ServiceWatch collector servers.

Per-Service Data Gathering

Customer must complete one **ServiceWatch Business Service Data Gathering Template** per business service to be modeled during the QuickStart prior to the start of this QuickStart implementation.

Technical Definitions

Please refer to the ServiceNow Wiki for technical definitions for the ServiceNow applications and platform at http://wiki.service-now.com.

Packaged Service Terms and Conditions

Based on the scope of services and assumptions set forth above, the services herein shall be performed on a fixed price basis plus expenses stated on the ordering document. Customer agrees to pay the total fee amount on the ordering document regardless of the total number of effort days ServiceNow takes to complete the project. ServiceNow will provide the services as described herein limited to those ordered on the ordering document: (i) if Customer is purchasing directly from ServiceNow, on the terms and conditions in the Order Form and the Master Ordering Agreement incorporated by reference herein from http://www.servicenow.com/schedules.do; or (ii) if Customer is purchasing from a ServiceNow authorized reseller (“Reseller”), on the terms and conditions in the use authorization as issued by ServiceNow and the Subscription Service Agreement incorporated by reference herein from http://www.servicenow.com/schedules.do. ALL ORDERS ARE NON-CANCELLABLE, NON-REFUNDABLE, AND NOT SUBJECT TO ACCEPTANCE. ALL SERVICES WHEN ORDERED AND ACCEPTED BY SERVICENOW MUST BE CONSUMED WITHIN 12 MONTHS FROM THE EFFECTIVE DATE OF THE ORDERING DOCUMENT. SERVICES ARE NOT INCLUDED IN THIS OFFERING UNLESS SPECIFICALLY IDENTIFIED AS INCLUDED IN THIS DOCUMENT. ANY PURCHASED AND UNUSED SERVICES SHALL EXPIRE WITH NO FURTHER CREDIT OR REFUND AND SHALL HAVE NO VALUE THEREAFTER. Customer shall reimburse ServiceNow or Reseller for all authorized, reasonable and verifiable travel expenses incurred during the performance of the professional services, training and other services.

For scheduled service days that are canceled or rescheduled by Customer with fewer than ten (10) business days prior written notice to ServiceNow, Customer shall be charged and pay for (a) any travel expenses that cannot be canceled or refunded, and (b) the canceled/rescheduled service days if ServiceNow is not able to reassign the personnel to another project. For the purposes of this section, email to the ServiceNow personnel assigned to this project will be sufficient as written notice.

Exhibit – ServiceWatch Implementation Prerequisites

This exhibit describes the credentials and connectivity considerations needed for the discovery process of ServiceWatch. ServiceWatch performs business service discovery without the use of agents. Therefore, ServiceWatch needs credentials to access the components to be discovered. ServiceWatch is built out of two (2) major components: a ServiceWatch server and a set of collector servers. The collector servers are the components that perform business service discovery and communicate the results to the ServiceWatch server over HTTPS. This architecture enables ServiceWatch to discover business services that span security zones.

The following are the requirements for a successful ServiceWatch implementation:

Client

For launching the ServiceWatch UI, a browser with Flash Player 10.1 or higher is needed. Internet Explorer (8 or higher), Mozilla Firefox and Google Chrome Browsers are supported.

Collector Server Requirements

Hardware

A dedicated server (virtual or physical) with the following minimum characteristics:

- 1 CPU
- 2GB memory
- 20GB disk space

Software

Customer will provide the following software loaded on each data collector server:

- Windows 2008 R2 64 bit
- .Net framework version 3.5 SP1

Business Service System Operating System Credentials

For ServiceWatch discovery to work the following business service system server credentials are needed:

- Windows servers: access is done via WMI and an administrator user is required (either local admin or domain admin)
- UNIX servers: access is done via SSH with either of the following credentials:
  - Non-root user & password and using the 'sudo' utility to run selected commands as root
  - Non-root user & password + root password for running selected commands with 'su'
  - Root user & password
- A certificate and optionally a passphrase may be used in addition or instead of a password for UNIX servers

Network Configuration

The collector(s) within Customer's network need to be able to initiate communication to ServiceNow's ServiceWatch network at address servicewatch.servicenow.com on port 443 (using HTTPS protocol).

Optionally, the collector may use a proxy to communicate with the host server (if such proxy exists) using either basic or NTLM authentication.

Network Device Credentials

Access to network devices (like load balancers or routers) is done via SNMP v1/v2c/v3 and a read only community string is needed (or proper credentials for SNMPv3). The network devices should be configured to allow SNMP access from the ServiceWatch server, in case access lists are active.

Virtualization Credentials

- VMware: a user with read only permission is required for access to VMware vCenter
- Citrix Xen: a user with read only permission is required for access to Citrix XenCenter
- Solaris Zones: OS level credentials (as defined above) are required for each global zone

AIX LPARs

In order to discover virtualization on AIX systems, we require the following credentials:

Access to HMC (Hardware Management Console)

A user that can login to the HMC and run the following commands:

- lssyscfg
- lshmc

Access to VIOS (Virtual I/O Server)

A user that can login to the VIOS and run the following commands via sudo:

- /usr/ios/cli/ioscli lsdev
- /usr/ios/cli/ioscli lsmap
- lstcpip

Specific Application / Device Level Credentials

The following applications and/or devices require additional credentials.

F5 Load Balancer

In addition to SNMP access, when using iRules, a read only BigIP shell user is required to access the load balancer over SSH.

Cisco ACE

A read only user with a network monitor role is required to access the load balancer over SSH.

Microsoft SharePoint & SSRS (SQL Server Reporting Server)

A user that has permissions within SharePoint/SSRS to access the administration page is required.

Microsoft CRM

The operating system user must be an administrator within CRM.

Websphere MQ

An operating system user like mqm is required, that can run commands like runmqsc or dspmq.

Microsoft SSIS (SQL Server Integration Server)

The user used by ServiceWatch should be an administrator of SSIS.

Microsoft Exchange

The user used by ServiceWatch should be an administrator of Exchange. For versions 2010 and above, an application level user and password to the admin page are required.

Microsoft NLB (Network Load Balancing)

ServiceWatch requires a password for remote administration (which should be enabled).

Oracle RAC

The user used by ServiceWatch should be able to run the crs_stat command using sudo.

Tibco EMS

An application level user and password to Tibco EMS are required to be able to authenticate to command lines like tibemsadmin.

Websphere Data Power

Read only user within Data Power that has access for all the domains and can run commands via SOAP. Read only community for access through SNMP.

Citrix XenApp (version <= 4.5)

Permission to access XenApp from VBscript

Citrix XenApp (version > 4.5)

Permission to access XenApp from PowerShell

Storage Prerequisites

Network Appliance Filer Storage Array

A read only user for login through HTTP to the NetApp Filer is required to read all configuration data (e.g. volumes, aggregates, network, HBAs, shares, etc.). The following are the specific capabilities that are required:

- login-http-admin
- api-system-get-info
- api-disk-list-info
- api-lun-list-info

- api-aggr-list-info
- api-volume-list-info
- api-cifs-share-list-iter-start
- api-cifs-session-list-iter-start
- api-cifs-session-list-iter-next
- api-nfs-exportfs-list-rules
- api-fcp-adapter-initiators-list-info
- api-fcp-adapter-list-info
- api-lun-map-list-info
- api-cifs-share-list-iter-next

Also, there needs to be read only SNMP access to the NetApp Filer.

EMC Symmetrix Product Line (Symmetrix/DMX/VMAX)

An installation of SYMCLI should be available on a server that is connected to all Symmetrix storage arrays.

The operating system user has to be able to execute the following SYMCLI commands:

- symcfg
- symdev
- symmaskdb
- symaccess

EMC Control Center (ECC)

Access to EMC ECC is done using queries to the ECC repository, therefore a username and password to the ECC Oracle repository is needed.

Network Connectivity

Host to collector communication

Windows host

The ServiceWatch collector is communicating with hosts using WMI (Windows Management Instrumentation) which runs on top of RPC. This means that the host may allocate ports in the range of 1024-65535 arbitrarily.

If the collector is located across a firewall from the host we have three options:

1. Open the firewall for ports 135,1024-65535
2. Configure the server to make WMI work with fixed port (http://support.microsoft.com/kb/897571/)
3. Place an additional collector in the zone of the host

If option 1 or 2 is selected, the following additional ports should be opened in the firewall:

- Access to admin share (e.g. C$) and TCP port 445 open (SMB over TCP port)
- HTTP access from the host to the collector. By default access is on port 8585 (configurable).

Unix/Linux host

SSH port (TCP port 22, configurable) should be open from collector to host.

Network devices

SNMP port (UDP port 161 by default, configurable) should be open from collector to host.

Collector to Server Communication

Collector communicates with the server using HTTPS on port 8443. Port 8443 should be open for communication initiated by the collector. This port is configurable and can be changed.

Browser to Server Communication

UI communicated with the server using HTTPS. By default we use port 8080 (configurable).

Server to 3rd Party Systems

VMware vCenter: ServiceWatch communicates with vCenter using HTTPS (port 443).

Citrix XenCenter: ServiceWatch communicates with XenCenter using HTTP over port 80.

Sudo Configurations on Unix Systems

Linux

The following commands are used via sudo on Linux:

- cat
- ls
- netstat (when executed not as superuser the command does not return the process ID)
- dmidecode (getting serial number of a machine) – optional
- gcore

Below is an example line in the sudoers file:

- qauser ALL=/bin/netstat, /bin/cat , /bin/ls, /usr/sbin/dmidecode, /usr/bin/gcore

Additional commands are needed for storage discovery:

- dmidecode
- fdisk
- iscsi-ls
- lvs
- lspci
- find /sys/class/scsi_host/ -name 'port_name' -print -exec cat {} \;

- find /sys/block/ -name device -exec ls -l {} \;

If a certain command exists in several places on the machine, ServiceWatch will use the following search path to find it. The sudoers file should be updated accordingly:

- /usr/local/sbin
- /usr/local/bin
- /sbin:/bin
- /usr/sbin
- /usr/bin

Solaris

The following commands are used via sudo on Solaris:

- cat
- chmod +x /tmp/nbltmp/inq) (only if storage is needed)
- gcore
- ifconfig (if not executed as super user, it doesn't bring the MAC addresses)
- ksh
- ls
- mdb (in global zone only)
- pwdx
- pargs
- /usr/ucb/ps
- zonecfg (in global zone only)
- Either of:
    - dtrace
    - lsof

Additional commands are needed for storage discovery:

- fcinfo
- isainfo (only if storage is needed)
- iscsiadm list – only if iSCSI is being used
- vxdisk list – only if Veritas Volume Manager is installed
- find /sys/class/scsi_host/ -name 'port_name' -print -exec cat {} \; – only if Emulex HBA is used
- find /sys/block/ -name device -exec ls -l {} \; – only if Emulex HBA is used

Below is an example line in the sudoers file:

- qauser ALL=/usr/bin/mdb, /usr/bin/pwdx, /usr/bin/pargs, /sbin/ifconfig, /usr/bin/ls, /usr/bin/cat, /usr/bin/chmod +x /tmp/nbltmp/inq (for storage detection only) , /usr/bin/gcore, /usr/bin/isainfo

Note: if relevant applications are running on Solaris local zone, same access rights should be provided on the corresponding global zone.

AIX

The following commands are used via sudo on AIX:

- cat
- gencore
- ls
- ps
- procwdx (get working directory of a process)
- rmsock (find process listening on a specific port)
- bootinfo (find the architecture of a server, i.e. 32/64 bit) – optional

Below is an example line in the sudoers file:

- qauser ALL=/bin/procwdx, /bin/cat , /bin/ls, /usr/sbin/rmsock, /usr/bin/ps, /usr/sbin/gencore

HP-UX

The following commands are used via sudo on HP-UX:

- cat
- ls
- Either of:
  - pfiles
  - lsof